EXAMINER'S AMENDMENT/COMMENT

Allowable Subject Matter

Claims 1, 3, 14, 16, 42-45, 47, 48, 51-54, and 58 are allowed.

The following is an examiner's statement of reasons for allowance: the prior art of record does not teach or suggest a combination as claimed, including wherein a monitor/regulator integrally disposed in a routing device of a first network domain or coupled to the routing device monitors network traffic routed by the routing device and/or a second routing device by analyzing flow records, each describing traffic conversation as indicated by a combination of source and destination addresses, received from the routing device, the monitor/regulator determining if the first network domain is sourcing undesirable network traffic, including network traffic sourced directly out of the first network domain and also including network traffic sourced originally from third parties and subsequently going through the first network domain, the undesirable traffic comprising a denial of service attack, wherein said monitor/regulator makes said determination based at least in part on differential characteristics between request packets routed out of the domain and response packets routed into the domain, wherein said monitor/regulator instructs the first routing device and/or said second routing device to lower a priority of the undesirable network traffic, wherein said monitor/regulator monitors a second network domain, and wherein said monitor/regulator, upon making said determination, lowers threshold criteria it uses to conclude that undesirable network traffic is being sourced out of the second network domain, as recited in each of the independent claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Grant Houston (Reg. No. 35,900) on April 12, 2011.

The application has been amended as follows:

IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in this application:

1. (Currently amended) A network comprising:

a first network domain;

a first routing device at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric;

a second routing device for routing network traffic out of and into the first network domain; and

a monitor/regulator, either integrally disposed in said first routing device or coupled to the first routing device to monitor the network traffic routed by said first routing device and said second routing device by analyzing flow records, each describing a traffic conversation as indicated by a combination of source and destination addresses, received from the first routing device and the second routing device, the monitor/regulator determining if the first network domain is sourcing undesirable network traffic, including network traffic sourced directly out of the first network domain and also including network traffic sourced originally from third parties and subsequently going through the first network domain to the first routing device, the undesirable network traffic comprising a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of or going through the first network domain based on the network traffic being routed by said first routing device and said second routing device,

wherein said monitor/regulator makes said determination based at least in part on differential characteristics between request packets routed out of said first network domain and response packets routed into the first network domain based on aggregated network traffic routed by the first routing device and the second routing device, and wherein said monitor/regulator instructs the first routing device and said second routing

device to lower a priority of the undesirable network traffic that is being sourced from or going through the first network domain[[.]],

wherein said monitor/regulator monitors a second network domain, and

wherein said monitor/regulator, upon making said determination, lowers threshold criteria it uses to conclude that undesirable network traffic is being sourced out of the second network domain.

2. (Cancelled)

3. (Previously presented) The network of claim 1, wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said first network domain by said first routing device and said second routing device, and aggregated statistics of said network traffic routed into the first network domain by said first routing device and said second routing device.

Claims 4-13. (Cancelled)

14. (Currently amended) A network traffic regulation method comprising:

monitoring, by a monitor/regulator, network traffic routed by a first routing device of a first network domain;

monitoring, by the monitor/regulator, network traffic routed by a second routing device of said first network domain;

determining, by the monitor/regulator, if the undesirable network traffic is being sourced directly out of the first network domain or is sourced originally from third parties and subsequently passing through the first network domain to the first routing device, the undesirable network traffic comprising a denial of service attack in which the undesirable network traffic is launched against [[to]] a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, wherein the first network domain is determined to be sourcing or passing through undesirable network traffic by analysis of flow records describing traffic

conversation, as indicated by a combination of source and destination addresses, received from the first routing device and the second routing device, which are positioned at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric;

wherein said determining comprises determining based at least in part on differential characteristics between request packets routed out of said network domain and response packets routed into the network domain based on aggregated network traffic routed by the first routing device and the second routing device; ~~and~~

wherein said monitor/regulator instructs the first routing device and the second routing device to lower[[ing]] a priority of the undesirable network traffic that is being sourced from or passing through the first network domain and routed by said first network device and said second network device[[.]],

wherein said monitor/regulator monitors a second network domain, and

wherein said monitor/regulator, upon making said determination, lowers threshold criteria it uses to conclude that undesirable network traffic is being sourced out of the second network domain.

15. (Cancelled)

16. (Previously presented) The method of claim 14, wherein said determining comprises inferring said differential characteristics based on aggregated statistics of said network traffic routed out of said first network domain by said first routing device and said second routing device, and aggregated statistics of said network traffic routed into the first network domain by said first routing device and said second routing device.

Claims 17-41. (Cancelled)

42. (Currently amended) The network of claim 1, wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics

.

43. (Currently amended) The network of claim 1, wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics.

44. (Currently amended) The network of claim 1, wherein said monitor/regulator generates statistics concerning distributions of time to live values and determines whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics.

45. (Currently amended) The network of claim 1, wherein said monitor/regulator tracks differences between outbound transmission control protocol (TCP) synchronize (SYN) and finish (FIN) packets and inbound response packets and determines whether the first network domain is sourcing or passing through undesirable network traffic based on said differences.

46. (Cancelled)

47. (Previously presented) The network of claim 1, wherein said monitor/regulator instructs said first routing device and said second routing device to slow the undesirable network traffic.

48. (Currently amended) A network comprising:

a first network domain;

a second network domain;

a first routing device at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric; and

said second network domain including a second routing device for routing network traffic out of and into the second network domain;

a monitor/regulator that monitors the network traffic routed by said first routing device and said second routing device by analyzing flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the first

routing device and the second routing device, and determines if undesirable network traffic is being sourced out of the first or the second network domains or is sourced originally from third parties and subsequently passes through the first or the second network domains, based on network traffic characteristics observed of network traffic routed through said first and second routing devices; the undesirable network traffic comprising a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of or going through the first network domain or the second network domain, based on the network traffic being routed by said first routing device and said second routing device,

wherein said monitor/regulator makes said determination based at least in part on differential characteristics between request packets routed out of each network domain and response packets routed into each network domain based on aggregated network traffic routed by the first routing device and the second routing device, and wherein said monitor/regulator instructs one of said first routing device and said second routing device to lower a priority of the undesirable network traffic that is being sourced from or going through the first network domain or the second network domain; and

wherein said monitor/regulator, upon ~~determining said undesirable network traffics~~determining that one of said first and second network domains is sourcing undesirable traffic, lowers [[a]] threshold ~~for concluding~~criteria it uses to conclude that undesirable network traffic are being sourced out of an other one of the first or the second network domains including being sourced originally from third parties and subsequently passing through the first or the second network domains.

49-50. (Cancelled)

51. (Currently amended) The method of claim 14, further comprising generating statistics concerning destination addresses and determining whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics.

52. (Currently amended) The method of claim 14, further comprising generating statistics concerning lengths of packets and determining whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics.

53. (Currently amended) The method of claim 14, further comprising generating statistics concerning distributions of time to live values and determining whether the first network domain is sourcing or passing through undesirable network traffic based on said statistics.

54. (Currently amended) The method of claim 14, further comprising tracking differences between outbound TCP SYN and FIN packets and inbound response packets and determining whether the first network domain is sourcing or passing through undesirable network traffic based on said differences

55-57. (Cancelled)

58. (Currently amended) A network comprising:

a network domain which is a local area network;

a routing device in the local area network at a boundary between the local area network and public internetworking fabric to route network traffic between the network domain and the public internetworking fabric; and

a monitor/regulator, either integrally disposed in said routing device or coupled to the routing device, to monitor the network traffic routed by said routing device by analyzing flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device, the monitor/regulator determining if the network domain is sourcing undesirable network traffic, including network traffic sourced out of the network domain and also including network traffic sourced originally from third parties and subsequently going through the network domain to the routing device, the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing or passing through the undesirable

network traffic, wherein said monitor/regulator instructs the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic;

wherein the undesirable network traffic comprises a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the network domain,

wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of or passing through said network domain relative to network traffic routed into said network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain and wherein said monitor/regulator instructs the routing device to lower a priority of the undesirable network traffic that is being sourced from or passing through the network domain[[.]],

wherein said monitor/regulator monitors a second network domain, and

wherein said monitor/regulator, upon making said determination, lowers threshold criteria it uses to conclude that undesirable network traffic is being sourced out of the second network domain.

59. (Cancelled)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER D. BIAGINI whose telephone number is (571)272-9743. The examiner can normally be reached on weekdays from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Biagini
(571) 272-9743

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2445